Mitigating Teredo Rooting Loop Attacks

(draft-gont-6man-teredo-loops-00)

Fernando Gont
on behalf of
UK CPNI

IETF 79
November 7-12, 2010. Beijing,China.

Summary

- **Aims at mitigating the Teredo routing-loop attacks described by the USENIX-WOOT paper (Nakibly et al)**
- **Discusses both implementation considerations and operations considerations**
- **Sanity checks are recommended for Teredo nodes (already implemented in some Teredo implementations), such that the vulnerabilities are eliminated**

Attack #1: Teredo client to NAT

- **The routing loop involves a Teredo client and the corresponding NAT (it assumes that the NAT is of type "cone", and that the aforementioned NAT supports hair- pin routing with source address translation**
- **Implementation advice:**
  - **a node SHOULD NOT forward over the Teredo tunnel IPv6 packets that were not originated on the local node, and SHOULD discard those packets received over the Teredo tunnel that are not destined to the Teredo client.**
- **The proposed checks completely eliminate this vulnerability.**

Attack #2: Teredo server

- **The routing loop involves only a Teredo server, having the server send a bubble packet to itself (resulting in an endless loop)**
- **Implementation advice:**
  - **Teredo servers MUST discard Teredo packets that have an IPv4 Source Address equal to one of the receiving server's IPv4 addresses, and MUST discard Teredo packets that embed the (obfuscated) IPv4 address of the receiving server in the "client IPv4" field of the Source Address or the Destination Address of the encapsulated IPv6 packet.**
- **The proposed checks completely eliminate this vulnerability.**

Moving forward

- **Comments?**
- **Adopt as wg item?**